TS4/FULL/19

4/9/19 (Item 15 from file: 148)

08120881 SUPPLIER NUMBER: 17376639 (THIS IS THE FULL TEXT)
How to keep your donors. (nonprofit organizations)
Himes, David P.
Fund Raising Management, v26, n6, p34(3)
August, 1995
ISSN: 0016-268X LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1604 LINE COUNT: 00131

ABSTRACT: Many nonprofit organizations are having difficulty finding new donors. This makes it even more important for nonprofit organizations to maintain their existing donors and to encourage them to continue giving donations. This can be done by managing well the process that happens after a donor gives a donation, such as acknowledging all donations and gifts in a timely manner, replying to all correspondence, offering a toll-free number to be used by donors to get more information or to complain, paying special attention to the accuracy of mailings and being prepared to send informational materials.

TEXT:

Good - even outstanding - customer service is no longer a luxury, it's a necessity for the successful non-profit to sustain proper funding from a large base of donors.

Are you having a hard time finding new donors? Welcome to the club, so is nearly everyone else.

Are you having a hard time keeping your previous donors active and giving? Welcome to the club, so is nearly everyone else.

Sure, you can name some exceptions to one or both of these conditions - most likely, they are exceptions because of "what's hot" on the evening network news or on the front page of the newspaper.

There are a few organizations who are attracting new donors effortlessly, thanks to that kind of "free" publicity and notoriety.

But even though it's true for some non-profits, you should find some consolation in the fact that it won't last. As soon as the broadcast media gets distracted by some other "hot" news, their "surge" of new donors will decline or completely die off.

Of course, these unpredictable windows of opportunity for significant donor acquisition programs lead to important changes in fund-raising strategy for any organization which relies heavily on direct-response fund raising. The most important part of any fund-raising strategy today is to (1) be ready for a massive donor acquisition effort, when your turn to be in the headlines finally comes and TABULAR DATA OMITTED| (2) keep the donors you have.

Getting into the headlines is not always under your control. Sometimes, you can influence it, but rarely can you control it. So, let's move onto strategy number 2: Keep the donors you have.

There is much more you can do to keep the donors you have, but it may require you to begin thinking in new ways. This has been emphasized to me in two presentations I heard recently. The first was by Russ Reid, president of the Russ Reid Company, when he presented a survey entitled, "The Heart of the Donor," to the DMA's Non-Profit Day in Washington, DC, in January 1995.

The first thing you have to learn is not to think just about your solicitations, but rather about the donor's response, desires, motivations and needs.

But I'm getting ahead of myself. Let's back up for a moment.

If you're having a hard time attracting new donors, then it goes without saying you want to do a better job of keeping your donors. You want to improve donor retention, reduce the donor attrition rate, increase the donor renewal rate, increase the lifetime value of a donor - all those good things.

But how do you do those things?

Historically, the solution to these objectives has been to better manage the solicitation process. Create more and better mailings. Stage more attractive events. Expand personal solicitation efforts. And those will have a positive effect. However, the constantly increasing levels of competition for your donors' contributions are going to limit how much this strategy can do for you.

Well, there is another way. Here is how Reid phrased it in his report on The Heart of the Donor: "Probably the single most important insight we gained from this study is that the central motivations of donors are personal and unique to each individual. And to truly understand what our donors care about - as individuals rather than as a group - we have to ask them, one by one. Equally important, we have to begin using this information in a personal way, by marketing to each donor as an individual. And by listening to each donor as an individual."

But how can you solicit 100,000 donors and treat each one as an individual - obviously, this means more than just personalizing the letter.

The answer lies in what many of us old-timers in the direct-response business call the back-end - what happens after someone actually responds to one of your solicitations.

For years, most fund raisers have focused on the back-end as a necessary evil. You have to do it, but just keep the cost low and get it done quickly.

However, reinvesting in the back-end - in customer service - may be the key to individual attention Reid highlighted when he recognized the value of the individual donor.

Notice the table above. It assumes (1) a new donor costs you $40, (2) you receive on average 2.5 gifts from each donor each year and (3) you spend $1.00 on the back-end, for each gift you receive. However, if you increased your back-end budget by 25 percent to $1.25 per gift, look what happens if the attrition rate drops. You don't have to find as many new donors and you can actually reduce your expenditures on donor acquisition-savings thousands of dollars a year. And you'll do even better, because your average number of gifts per donor per year will probably increase - which this table doesn't even address.

But what can you do to improve the back-end and the customer service components of what you do? Here is my list:

1. Offer the donor more ways to contribute - let them pick the method most convenient to them - paper check, electronic check, credit card. Don't make a big deal out of these options. Most people will continue to give with paper checks, but the other options are growing in popularity, especially for monthly giving programs.

2. Acknowledge all gifts immediately - send a thank-you letter within 48 hours of receipt. Within 24 hours is better, but is unrealistic for most organizations - and really unnecessary, as well.

3. Fulfill all premiums within 48 hours - if it's important enough to offer it's important enough to mail it back to your donor promptly. It's probably even more important than the thank-you letter.

4. Reply to all correspondence with at least an acknowledgment of its receipt and a substantive reply if warranted. Few organizations handle donor correspondence well. So, if you do, you will really stand out.

5. Offer an 800 number where donors can call for more information or even to complain. And don't worry about the complaints. Think about it: If your donors didn't care enough to complain, they don't care enough to give.

The fact someone complains means they want to maintain a good relationship with you, but they're having trouble doing it right now - help them keep the good relationship with you. Help them get over the trouble - whatever it is.

6. Be prepared to send information in a variety of ways - fax, e-mail, computer bulletin board, overnight mail. You should develop a wide range of reports on all aspects of your activities. A newsletter is the most common information vehicle, but don't limit yourself to just a newsletter.

7. Pay special attention to the accuracy of your data - this includes, but should not be limited to, name, address, phone numbers, giving transaction data and all other data you maintain on your donor database. Few things are more needlessly annoying to a donor than to try three or four times to get their name or address corrected.

Many non-profits have limited their view of the back-end to caging and thank-you letters. For many years, that was enough. But it's not any more, the back-end includes a lot more, or at least it should. And if it doesn't mean that to your non-profit - look out!

You need to begin thinking about customer service for your donors - call it donor service, member service, partner service - whatever is the proper term for your donors. But it's more than just getting a donation into the bank and then getting a thank-you letter out six weeks later.

And you don't have to do all this yourself. Look outside for vendors who can help you. Reader's Digest outsources nearly all of its order processing and customer service. So do some of the largest non-profit associations in the country. You don't need to build a huge internal staff remember what Peter Drucker said, "Know your business."

Do what you do best and hire someone else to do what they can do best. Your business is providing help and services to your primary constituents.

But don't forget, good - even outstanding - customer service is no longer a luxury, it's a necessity for the successful non-profit to sustain proper funding from a large base of donors.

From another point-of-view, what you need to do is find a way to treat every donor the way you treat your biggest donor. That's quite a challenge. But here is what will happen if you succeed:

Your donors will perceive increased value of their contributions. Your donors will perceive increased appreciation of their contributions. Your donors will perceive increased need for additional contributions. More of your donors will give more often. Your donors will perceive a greater effectiveness in achieving results in your area of activity. You'll reduce fund-raising costs by improving the quality and accuracy of donor database. You'll increase the flow of information to your donors.

8. Your donors will continue to give to your organization for a longer period of time. The cumulative effect of these will have a dramatic and positive effect on all your fund-raising activities.

If you'd like some stimulating reading on a similar topic, I recommend, "The One To One Future," by Don Peppers and Martha Rogers. It is an excellent book on how to develop a one-to-one relationship in the context of direct-response marketing to a large audience.

David P. Himes is senior vice president for planning and development at the AB&C Group. He has served as administrator for an educational non-profit and deputy director of finance and administration for the National Republican Committee. He has additional experience in direct mail fund raising for colleges, universities, and charitable groups such as March of Dimes, American Red Cross, St. Judes Children's Hospital and the American Cancer Society.

SPECIAL FEATURES: illustration; table
INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting
DESCRIPTORS: Fund raising--Technique; Nonprofit organizations--Public

```
  relations
 PRODUCT/INDUSTRY NAMES:  8380000 (Nonprofit Institutions)
 FILE SEGMENT:  TI File 148
?
```

TS4/FULL/15

4/9/15 (Item 11 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08224217 SUPPLIER NUMBER: 17420572 (THIS IS THE FULL TEXT)
E-banking: FSTC unveils electronic check technology - secure, versatile instrument for electronic commerce. (Financial Services Technology Consortium's Electronic Check system)
EDGE, on & about AT&T, v10, n374, p41(1)
Sep 25, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 723 LINE COUNT: 00075

TEXT:

A consortium of major North American banks and computer firms, Thursday successfully completed a coast-to-coast all-electronic check transaction over the Internet.

The Electronic Check technology is being developed by the Financial Services Technology Consortium (FSTC). "Not only did the demonstration work successfully, but we demonstrated that this group can successfully work together to develop a common technology infrastructure for the common good of our industry and the customers its serves," said John Doggett, FSTC project director and director of applied technology at Bank of Boston.

The technology provides consumers and businesses of all sizes a common, secure and portable payment method that operates similarly to the way paper checks do -- "except better," Doggett said. Benefits of FSTC Electronic Check system include:

* Modeled on paper check, providing ready acceptance and ease of use.
* Strong security and fraud prevention.
* Checks can be written spontaneously by individuals or businesses.
* Provides complete verification and fully automated payment processing.
* Reduces manual check processing.
* Designed to integrate into today's PC applications and bank systems.
* Reduces fraud potential using automated digital signature verification.

This demonstration involved buying gift items over the Internet using Electronic Checks for payment that were deposited electronically via electronic mail into the merchant's account at the Bank of Boston, and paid from the buyer's account at Chemical Bank in New York. The actual financial settlement was accomplished by clearing the Electronic Check transactions through the Automatic Clearing House system. Each time the Electronic Check changed hands, the system's technology automatically verified that the check was genuine.

The Electronic Check uses standard cryptographic techniques to create a digital signature and a tamper-proof document. To ensure maximum security in the system, Electronic Checks are generated from Electronic Checkbooks using a PC card or smart card. These checkbooks, which must be unlocked using a PIN or password, provide "blank" checks, a check register, and safe, tamper-resistant and portable storage for the cryptographic keys used to sign and secure the Electronic Checks.

During first-ever public demonstration of the Electronic Check, a gift was purchased for Vice President Al Gore, who is widely known as a proponent of the Information Superhighway.

"The Electronic Check system fills a void in meeting the payment needs of customers and businesses wanting to complete electronic business transactions," said John Fricke, vice president of Texas Commerce Bank, a unit of Chemical. "Our system brings together the trusted bank

infrastructure that exists today and the broad reach of the Internet, to provide a secure alternative to paper-based payments," added Fricke, who heads the Electronic Check business team.

"We are building a robust, open system that can accommodate a broad range of product and technology developments," said project manager Frank Jaffe of Bank of Boston. "The resources and expertise made available to FSTC by the participating organizations, and the high level of individual cooperation within the team, enabled us to complete this demonstration in just five months." According to Bellcore's Milton Anderson, who heads the Electronic Check technical team, "the major technological breakthrough is the use of hardware-based cryptographic signatures to identify the writer and endorser and to secure the Electronic Check's content as it moves through the entire process of being verified, endorsed and cleared."

"Our goal is to extend the existing familiar payment system to enable electronic commerce over public networks, providing a cost-effective, secure, trusted alternative to credit-based transactions," Doggett added. More consumers and businesses are conducting electronic commerce today, and this new system will accommodate this growing interest with its security features and versatility -- e.g., direct and other deposits, and other forms of check including foreign currency checks and certified checks. Bank members of the FSTC Electronic Check program are: Bank of America, Bank of Boston, Bank of Montreal, Bank One, Chemical Bank, Citibank, Huntington Bancshares, and Wells Fargo Bank. Industry members are: BBN Inc. (Bolt Beranek & Newman), Equifax, IBM Corporation, IRE (Information Resources Engineering Inc.), National Semiconductor, Sun Microsystems and Telequip. Research and consulting organization members are: Bellcore, Oak Ridge and Sandia National Laboratories, and the University of Southern California-Information Sciences Institute. Advisory members are: Electronic Check Clearing House Organization (ECCHO), National Automated Clearing House Association (NACHA), and Intranet. Formed in September 1993, FSTC is a consortium of some 65 organizations, comprising banks, financial services firms, industry partners, national laboratories, universities, and government agencies. FSTC sponsors collaborative research and development on technical projects affecting the entire financial services industry and its users with particular emphasis on projects involving electronic commerce. Other FSTC projects include interbank check imaging, electronic commerce, and fraud detection and management.

INDUSTRY CODES/NAMES: TELC Telecommunications
DESCRIPTORS: Electronic data interchange--Research
PRODUCT/INDUSTRY NAMES: 4811500 (Specialized Telecom Services)
SIC CODES: 4822 Telegraph & other communications
FILE SEGMENT: CD File 275
?

TS4/FULL/13

4/9/13 (Item 9 from file: 148)

08848770 SUPPLIER NUMBER: 18544837
Electronic checks - a detailed preview.
Doggett, John
Journal of Retail Banking Services, v18, n2, p1(10)
Summer, 1996
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4970 LINE COUNT: 00418

ABSTRACT: Electronic checks constitute a new form of retail payment system developed by the Financial Services Technology Consortium to meet the demands of fast commercialization and public network growth. They provide swift,convenient and secured payments of financial accounts via public networks without the need for prearranged transactions. Electronic checks are delivered by direct transmissions or by public electronic systems.

TEXT:

...a totally new form of consumer payment system promises to dwarf all others in its convenience, flexibility, and security....The electronic check is...an innovative, all-electronic, payments (as well as a deposit-gathering) instrument that can be initiated by an individual or a business from a variety of devices.

The physical payments systems are many today and have grown up to meet the payment and settlement needs of individuals and businesses. Payment instruments have evolved over time to address different trading requirements or preferences found in these common business relationships:

* individual to business,
* business to business,
* business to individual, and
* individual to individual.

In some of these situations - individual to individual, for example - only cash and checks are normally used. Between individuals and businesses, the most common payment methods are cash, check, credit card, and direct debit.

Each instrument is used or accepted according to the payer/payee preference or capability to handle the transaction. For example, credit card transactions are seldom, if ever, used for the transfer of value between individuals not in a business situation.

The paper check is a popular payment instrument, as evidenced by its volume and continued growth in use; in the U.S. last year, the volume of checks exceeded the combined volume of credit card, ATM/POS, ACH and electronic check presentment (ECP) transactions (ILLUSTRATION FOR EXHIBIT 1 OMITTED) in all trading situations by more than three to one.

Making a Purchase with a New Payment System

Last year, one trial transaction was successfully completed with a totally new form of consumer payment system that promises to dwarf all these others in its convenience, flexibility, and security - the electronic check.

The electronic check is being developed under the auspices of the Financial Services Technology Consortium (FSTC), formed in 1993 to perform cooperative research and development projects for the benefit of the financial services industry. The consortium focuses on infrastructure development initiatives. In the two years since its formation, FSTC has grown to over 80 member organizations including banks, financial services companies, technology suppliers, research organizations, government labs,

and universities. (The names of the member organizations can be found on the Consortium's web-site, http://www.FSTC.org.)

This is how the first electronic check transaction worked. While browsing PC Gifts and Flowers, a World Wide Web gift catalog "store" on the Internet, a member of FSTC selected a teddy bear to be purchased. The purchaser completed the electronic order information form on PC Gifts and Flowers' web site, and requested payment by electronic check.

An electronic checkbook - a small, portable, "smart" PC card - was inserted into a reader on the PC and opened using a password. (This password goes only between the PC keyboard and the PC card, not over the network.) Once opened, the PC card generated an electronic check, filled in the payee, amount, and date information, and displayed an image representation of the check on the PC screen. The digital signature as well as two electronic certificates for the account and issuing bank - Chemical (now Chase) Bank - were added to the electronic check form; the check and order form were then protected against tampering by the use of a secure hash algorithm process. The check was recorded in the "smart" PC Card in the card memory and transmitted to PC Gifts and Flowers.

PC Gifts and Flowers received the check and order form and validated the check signer's digital signature through the use of the customer's public key. In addition, the account number and Chemical Bank's certificate were similarly validated. With the check validated, the merchant proceeded to post his accounting system and endorse the check with his signature and bank certificates of his bank, the Bank of Boston.

When this was completed, PC Gifts and Flowers added an electronic deposit slip and e-mailed the check and slip to the Bank of Boston. The Bank of Boston received the e-mail package, validated the check for both payer and payee, and, with the instrument authenticated, wrapped the check in an ACH transaction for transmission and settlement with Chemical Bank. The transaction then appeared as an electronic ACH transaction on the FSTC's account. Chemical Bank also validated the check, contained within the ACH transaction, to assure that the check was authentically signed by its customer, FSTC. And the teddy bear was sent out.

Creating and Defining Electronic Checks

As part of the FSTC's work, development of the electronic check is a collaboration of over 30 organizations: banks, technology companies, and research groups. Following last year's trial purchase from the Internet gift store, several additional pilots are being planned to start later this year.

The electronic check will build upon as much existing work as possible. This new payments instrument is being designed to integrate with the existing infrastructure by refining the paper check process to take full advantage of the electronic medium, while at the same time seeking to address many of the deficiencies of the paper check.

The need for such an instrument is becoming clear. The rapid commercialization and growth of public networks, including the Internet with its estimated 30 million users, is creating a huge potential worldwide electronic marketplace. So it should not be surprising to find the development of similar electronic payment instruments in the emerging world of electronic commerce on the Internet. Digital cash has appeared; electronic credit cards, as well as the electronic check, are in development. All of these behave in a similar fashion to their real-world cousins.

The electronic check is an innovative, all-electronic, payments (as well as a deposit-gathering) instrument that can be initiated by an individual or a business from a variety of devices, such as a personal computer, screen phone, ATM, or payments accounting system. The electronic check provides rapid and secure settlement of financial accounts between trading partners over open public or proprietary networks, without requiring pre-arrangement, by interconnection with the existing bank

clearing and settlement systems infrastructure.

The electronic check is modeled on the paper check, except that it is initiated electronically, and uses a smart card as an electronic checkbook, a tamper-proof electronic document for the check, digital signatures for signing and endorsing, and digital certificates to authenticate the payer, the payer's bank and bank account. However, unlike the paper check, through the use of an issuer-defined parameter, the electronic check can resemble other financial payments instruments, such as electronic charge card slips, travelers checks, and multi-currency or certified checks.

Although the primary use of the electronic check is to make electronic payments on public networks, the design will enable electronic checks to be used in any situation where a paper check is used today. For example, banks will use electronic checks to gather electronic deposits from public network users, thus opening the opportunity for complete, full-service electronic remote banking, anywhere the customer is connected. Later, physical point-of-sale implementations are possible at the check-out counter, to provide a safer, more effective off-line debit instrument.

The electronic check is delivered by either direct transmission or by public electronic mail systems. Payments (deposits) consisting of electronic checks are gathered by banks via e-mail and cleared through standard banking channels, such as ECP or ACH networks. This integration of the existing banking infrastructure with the new, rapidly growing public networks in a secure fashion provides a powerful implementation and acceptance path for banking, industry, and consumers.

Business Process Model

The electronic check provides a generic model for all electronic, digitally signed and authenticated financial instruments. The electronic check model will replicate the paper check flow but it will also:

* enable new services by making possible new flows - e.g., the payee can verify funds availability at the payer's bank

* enhance security at each step of the transaction by enabling automatic validation of the electronic signature by each party (payee and banks)

* facilitate integration with electronic ordering and billing processes

The security/authentication aspects of the electronic check are supported via digital signatures using public key cryptography. Encryption is not required for fraud prevention purposes, although it may be used for privacy reasons. A mechanism is designed into the electronic check to prevent interception and fraudulent use of account numbers by eavesdroppers.

The electronic equivalent of the checkbook will provide:

* secure storage of the user's private cryptographic key, which is used to digitally sign electronic checks when they are written and endorsed

* a register of checks signed, endorsed, and issued, read by an outside software program via an Application Programming Interface (API)

Electronic checks can be used directly, or through third-party service providers. They can be exchanged consumer to consumer, consumer to business, business to consumer, and business to business. If the payer is a business, then the requirements for signing and logging capacity in the electronic checkbook are greater.

Functional Flows. The electronic check concept, since it is based on the existing paper check model, is fairly easy to understand. There are multiple scenarios for the functional flows of electronic checks, including:

The Deposit and Clear Scenario. Payer receives a bill/invoice from payee, issues an electronic check, and sends it to the payee. The payee presents the check to her bank which, in turn, will settle it with the payer's bank. This is the typical check flow and is illustrated in Exhibit 2.

The Cash and Transfer Scenario. Payer receives a bill/invoice from payee, issues an electronic check, and sends it to the payee. The payee presents it directly to the payer's bank to be paid to the payee's account at his bank (ILLUSTRATION FOR EXHIBIT 3 OMITTED).

The Lockbox Scenario. Payer receives a bill/invoice from payee, issues an electronic check, and sends it to the payee's bank, either directly or via a lockbox. The payee's bank then sends accounts receivable information to the payee and clears the payment with the payer's bank (ILLUSTRATION FOR EXHIBIT 4 OMITTED). In this scenario, there may be no payee endorsement.

The Funds Transfer Scenario. Payer receives a bill/invoice from her bank (assuming electronic bill presentment allows for capture of the payee's bills by the payer's bank), issues an electronic check, and sends it back to her bank. The payer's bank, in turn, transfers funds to the payee's account at the payee's bank (ILLUSTRATION FOR EXHIBIT 5 OMITTED).

Distinguishing Characteristics

The electronic check is being designed for maximum flexibility, security and reliability, and minimum cost. It has several, practical characteristics that make it unique.

Clearing Cycle is Asynchronous. There is no set schedule for clearing payment, since the payment can be passed at will to each holder in due course, like a paper check. The recipient of the electronic check determines when it is to be paid. The check could take a matter of hours or even days to clear through the financial systems. No on-line system is required and each holder can determine the most economical path for this payment to travel, making this form of payment potentially less expensive than alternatives.

Payment is self-contained. The packet of digital information which forms the electronic check is self-contained and possesses both data describing the payment and information necessary to process the payment. In addition, it contains security elements to enable the check and its signer to be authenticated and to provide detection for any tampering that might occur when it is passed from holder to holder. The payment then is not tied to any payments network or system, and so the market is freed to seek the least costly and most reliable method of value exchange.

No pre-existing arrangement is necessary. Electronic check payments do not require any pre-existing relationship between the payer and the payee. No third party is required, as in an electronic bill payment service. This should translate into significantly reduced cost for electronic bill paying, for example.

Transmission over public networks. Electronic check payments can be made over public networks such as the Internet, a radical departure from previous payment systems that require dedicated private networks. The use of e-mail for transmission gives the electronic check great flexibility and low cost.

Optional features: authorization and guarantees. Although not a standard function for the electronic check, pre-authorization (certified check) or check guarantee is easily incorporated into the flow design. Since it is not required, the trading parties can choose whether to add this cost to the transaction.

Technical Architecture: Key Design Objectives

The technical features of the electronic check are designed to further the basic goals of flexibility, convenience, and minimum cost.

Parameterized Electronic Payments Instrument. Through specification of attribute parameters and routing information, the secure electronic check format can assume the properties of other payment instruments - e.g., a credit card slip, a travelers check, electronic benefits transfer payment, and so on. The flexibility of this parametric approach enables multiple electronic payments instruments to meet current needs, while providing for new instruments.

Open Integration with Accounting Systems. The electronic check can be

attached to electronic remittance information provided by the remote trading partner. This enables the payment to be made, routed correctly, and automatically posted to both trading partners' accounting systems. Integration with micro-payment accounting systems for high-volume, small-value financial transactions will enable those systems to settle accounts using the electronic check. The standardization of the electronic checkbook interfaces and the APIs to access electronic checkbook functions will simplify integration with a variety of home and small-business accounting and communications software packages.

Open Integration with Existing Interbank Payments Mechanisms. The design of the electronic check allows for gateways between the public network and the financial networks that can filter out all undesired traffic. The cryptographically sealed and authenticated electronic check document becomes the integration point between the public networks and secured financial networks.

Authentication of Electronic Checks. Today, with paper checks, authentication can only be effectively done by the check issuer. But both electronic checks and their checkbooks can be authenticated by the use of public key certificates at any point in the settlement cycle by a merchant or a bank. Deposit slips, endorsements, and so on may be cryptographically linked to the original check as it is processed, resulting in an electronic document suitable for archiving and use as evidence of payment.

Fraud Prevention and Confidentiality. Security measures will eliminate most of the causes of losses due to bad checks, including forgery, alteration, duplication, and fraudulent depositing. Forgery will be prevented through ensuring that digital signature keys are stored in secure hardware devices, and through appropriate controls over the validity of electronic check certificates. Alteration will be prevented through the application of digital signatures to the electronic check, and through the use of the secure hash function, which creates a unique digest of the electronic document.

Duplication is a somewhat more difficult problem to prevent and this will be addressed in several ways. First, electronic checks will require a date, and will be designed to expire more rapidly than paper checks. Second, electronic check certificates will also expire, preventing their use after a given time period. Third, the issuer bank will keep an archive of electronic checks that have been presented previously. The combination of these efforts should effectively minimize the risk of a duplicate electronic check successfully flowing through the payments system.

Fraudulent depositing is another significant issue, since electronic checks that are sent unencrypted could conceivably be deposited or "cashed" by someone other than the intended recipient. The electronic check design will apply the intended recipient's cryptographic keys to minimize this problem. The project will also seek additional techniques in order to resolve this issue and any other security issues that arise.

In the event that an electronic checkbook is compromised - either lost, stolen, or repudiated by a customer - the certificates for that checkbook can be revoked. The electronic check project will identify the conditions and requirements for maintaining and using certificate revocation lists as part of the cryptographic infrastructure required to support electronic commerce activities.

Ensuring the confidentiality of critical customer information is a priority for any network payments instrument. Toward this end, the electronic check will not contain existing checking account numbers, which could be intercepted and then used to commit fraud by paper check. Other information typically found on a paper check, such as address, will be examined in detail, and where appropriate either omitted, or made optional. In addition, we expect that electronic checks and other parameterized payment instruments will be encrypted, where possible, during transfer between parties to ensure confidentiality.

Critical Technology Components

The technical components of the electronic check are the means of achieving the key objectives. Modularity offers flexibility, and various features ensure security.

Modular design. The modular design is based on a standard electronic check format and content, standard electronic checkbook interfaces, and standard API. The design also separates the cryptographic functions from the applications that write and endorse checks, both physically and logically, to facilitate application of this cryptographic infrastructure to secure other financial instruments or documents. The cryptographic infrastructure is used to authenticate the customer and account, electronic check document and issuing bank, and to securely seal the electronic check, enabling the use of public networks for transportation.

The electronic check concept makes use of two critical technology components:

* The electronic checkbook, a tamper-resistant signature card or other hardware to protect private keys

* Public key cryptographic signatures

The electronic check and electronic checkbook. One key innovation is to use an electronic checkbook to generate an electronic check. The electronic checkbook may be implemented as a tamper-resistant PC card, which contains a mechanism to generate or store unique check identifiers, to maintain a check register, and to calculate and verify digital signatures and certificates using public key cryptography. Alternatively, the electronic checkbook may be implemented in an ISO-format smart card (perhaps without the check register functions due to memory limitations) or it may be implemented in cryptographic hardware processors for use by systems that process large volumes of checks or that maintain a number of electronic checkbooks.

Public key cryptographic signatures. These signatures are used to sign checks when they are written, co-signed, endorsed and processed. Cryptographic signatures are also used to create "letters of reference" (cryptographic certificates) that allow a public signature verification key to be used to verify the signer's signature.

Public key cryptographic signatures are necessary because the signature of each signer, computed using the signer's private key, can be verified by anyone else who knows the signer's public key. This property is not shared by "test keys" or "message authentication codes" (MAC) computed using secret key cryptography. Consequently, only public key signatures are useful for electronic checks, which are successively signed and verified during processing; secret key MACs are not.

Since the signer computes his or her signature on a document using a private key, and since the verifier verifies the signer's signature using the signer's public key, there must be a way for the verifier to trust the association between the signer (and the signer's account information) and the public key used to verify the signer's signature on the electronic check. The signer can expedite the establishment of trust by enclosing with the signed check a "letter of reference" (cryptographic certificate) stating the signer's name, account number, and signer's public signature verification key, all signed by the bank holding the account. Similarly, a second "letter of reference" (certificate) can state the bank's name, bank details, and the bank's public signature verification key, all signed by a central body such as the Federal Reserve. Therefore, anyone knowing the Federal Reserve's public signature verification key can sequentially verify the bank's certificate, the account certificate, and then the signature on the electronic check.

Tamper. resistant signature cards or other hardware devices. These devices are needed to compute the signatures without the possibility of disclosing the signer's private signature key. If the private signature key is disclosed, then anyone can use it to forge the signer's signature. If

significant numbers of private keys are disclosed and are used to forge checks, then electronic checks will not be accepted, especially in applications where other identification is not present, such as electronic mail ordering, electronic shopping, and paying for information services.

Signature cards always keep the private key internal to the processor and memory on the card. The document to be signed is sent into the signature card, and the signature card uses the private key to compute the signature. The private key is never accessible via the card's connector. A similar function can be served by large-scale cryptographic processors, such as Atalla or Raced Dataguard boxes, for large operations where individual signature cards are impractical.

Tamper-resistance is needed to the extent necessary to make it economically unattractive for attackers to steal signature cards, extract the private key, and pass bad checks using the key before the card is reported stolen and the account closed. However, the degree of tamper-proofing required for some electronic money systems is not necessary, since the card only contains private information for one account (rather than system-level secrets) and since the card holder is incented to report theft or tampering (rather than to extract a secret to use for fraud or counterfeiting).

Modularity and Open Interfaces. The prototype and eventual production implementation of the electronic check concept will consist of interconnected modules providing services to other modules and to APIs. The APIs will provide electronic check services to user interface applications, to financial applications such as bill payment, and to third-party applications.

The applications and APIs needed for electronic checks are broken into multiple categories, including:

* Management
* Check writing
* Check acceptance and endorsement
* Check clearing
* Reconciliation

Management functions will allow for card issuance, inactivation, reactivation, and key management functions. Check writing is assumed to be performed by the payer, acceptance and endorsement by the payee, clearing by the banks, and reconciliation by the payer. Note that most users and organizations will assume the roles of both payer and payee, but at different times; thus, these two functions will be considered separately.

Beneath the modules implementing each of the functions just mentioned, a base set of supporting modules is also required. These base modules provide for the creation, destruction, and manipulation of a parameterized electronic financial instrument (the electronic check), the interpretation of such instruments as electronic checks, the generation and verification of digital signatures on the payment instruments, and the interaction with electronic checkbook hardware devices.

Benefits of Electronic Checks

The goal of all the various technological innovations discussed above is to create a new payment system with unique features and a variety of user benefits. Electronic checks enable banks to gather deposits electronically. Electronic checks address the problem of gathering deposits electronically over public networks, since all customers - retail and commercial - can gather, transmit, and deposit electronic checks into their accounts without physically going to a bank branch.

Electronic checks fill an electronic commerce payments void. Electronic checks address a gap, which banks can fill, in the payments infrastructure - specifically, the lack of an electronic payment alternative for trading using public data networks to conduct transactions.

Rapid adoption. The electronic check is an all-electronic payment instrument, modeled on existing paper check processes to enable it to be

readily accepted by the marketplace. By retaining the basic characteristics and flexibility of the paper check while enhancing the functionality, the electronic check can be adopted more rapidly.

Great flexibility. The electronic check design enables great flexibility, through support for other types of payment instruments - e.g., certified check, cashiers check, credit card charge slip, and so on - and added capabilities, such as future dating, limit checks, and multi-currency payments.

An efficient alternative for both consumer and corporation. The electronic check can be used advantageously in all market segments, from the individual consumer to the large corporation, as it will enable businesses to safely complete payments over networks in a more cost-effective manner than present alternatives.

Automated posting of accounting information. Since the contents of a check can be attached to the trading partner's remittance information, the electronic check will easily integrate with existing or new applications, such as accounts receivable. In addition, electronic checks can be integrated into other payments systems, such as micropayment billing systems and other emerging network payment alternatives.

A secure, trusted instrument. Building a secure, trusted, workable payments option for electronic commerce requires an in-depth understanding of the options, problems, and barriers to acceptance from the perspectives of consumers, businesses, and financial institutions. The use of digital signatures, hardware-based signing, and banks as certification agents, will make the electronic check trusted and secure.

Open integration with existing interbank payments mechanisms. The secure electronic check document enables open public networks to be linked to the financial payments and bank clearing networks in a secure fashion, leveraging the ubiquitous access of public networks with the existing financial payments infrastructure.

Authentication of electronic checks. Using public-key certificates enables electronic check authentication by the payee, and payee's and payer's banks, a feature that is not available today for paper checks. Digital signatures can be validated automatically, while today's paper checks require a manual process, which can only be done by the payer's bank, to compare handwritten signatures.

Fraud prevention and confidentiality. Electronic checks will be tamper-resistant due to the use of cryptographic signatures. This will provide greater security and reduced fraud losses for all parties in the payments process by eliminating most of the common causes of bad paper checks. To provide confidentiality, electronic checks may be encrypted when sent over public networks.

Standards. Except for electronic cash, none of the other payment methods actually affect final settlement or actual transfer of funds. In the case of the electronic check, only one standard is being proposed, backed by an impressive array of the nation's largest banks, and based upon many established financial industry and security standards. Also, the electronic check has much less risk than electronic cash, in that the holder would lack the incentive to commit fraud against his own account, lacking the ability to try to be his own mint. The card holds only check forms - not intrinsic value, such as cash.

Looking Ahead

The nature of the electronic check not only offers trading partners and consumers an attractive, flexible payments instrument, but also offers banks the ability to accept deposits over the Internet.

A number of pilot proposals are being considered in many different business situations. Brokerage, publishing, and technology component suppliers are just three areas which appear attractive. The business to business use is compelling, although another consumer retail trial is also planned. By next year, several trials should be under way.

The prospective scope of the electronic check is enormous - it can go potentially everywhere a paper check is used today. As electronic checkbooks proliferate, the use at physical points of sale, for example, will become common. Combination cards, with electronic check and credit card for greater convenience, are possible.

However, the prospect of mass usage of the electronic check within a year or two, while feasible, is unlikely. The pace of change in the banking industry has traditionally been slow. For example, ATMs have taken some 15 years to achieve a critical mass in the market, and credit cards took more than 20 years to do likewise.

So we would be doing well to find electronic checks in use in large numbers by the turn of the century. But the pace of technological change seems to have picked up in recent times - so any forecast will almost certainly be off the mark!

John Doggett is the Director of Applied Technology at the Bank of Boston. He is also the vice chairman and a member of the Executive Committee of the Financial Services Technology Consortium and a member of the Executive Committee of CommonWealth Exchange, a Massachusetts-based group of corporations exploring electronic commerce and inter-company collaborative work on the Internet.

The FSTC Electronic Check project is funded in part by the Advanced Research Projects Agency. No official endorsement should be inferred. The contents of this document do not necessarily reflect the policy of the U.S. government.

SPECIAL FEATURES: illustration; chart; graph
INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting
DESCRIPTORS: Electronic funds transfer systems--Evaluation; Payment--Innovations; Checks--Innovations
PRODUCT/INDUSTRY NAMES: 3573064 (Electronic Funds Transfer Systems)
SIC CODES: 3571 Electronic computers
FILE SEGMENT: TI File 148
?

BANKS, TECHNOLOGY COMPANIES PLAN `ELECTRONIC CHECK' SYSTEM

Seattle Post - Intelligencer; Seattle, Wash.; Aug 23, 1995; THE NEW YORK TIMES;

Sub Title: [FINAL Edition]
Start Page: B.8
ISSN: 0745970X

Abstract:
*The system would let a couple pay their phone bill by sending a payment to the telephone company over electronic mail, or they could send an **electronic check** to a child for a **birthday** present. A person or company receiving an **electronic check** could immediately deposit it in a bank, also by electronic mail.*

Full Text:

Pretty soon it won't be "The check is in the mail"; it will be "The check is in the e-mail."

A group of banks and technology companies said yesterday they would design a system to create "electronic checks" that could be used to make payments over the Internet or other electronic mail systems.

The system would let a couple pay their phone bill by sending a payment to the telephone company over electronic mail, or they could send an electronic check to a child for a birthday present. A person or company receiving an electronic check could immediately deposit it in a bank, also by electronic mail.

Unlike the electronic bill-payment services increasingly offered by banks, electronic checks could be sent directly by customers to their recipients without going through a bank.

The electronic check would contain all the information that is on today's paper checks, including a "digital signature."

To use the system, consumers would need an electronic checkbook, a card that would be inserted into a slot on their computers. The card, which is expected to cost $30 to $40 wholesale, would be required to verify the identity of the check writer.

The project is at an early stage, and such issues as pricing have not been determined. The group hopes to set up a small test with fewer than 1,000 participants next year.

You could soon be sending checks by E-mail // TECHNOLOGY: A group of banks and technology companies is designing `electronic checks.'

Orange County Register; Santa Ana; Aug 23, 1995; SAUL HANSELL: The New York Times;

Sub Title: [MORNING Edition]
Start Page: c.04

Abstract:
*A group of banks and technology companies said Tuesday that it would design a system to create "**electronic checks**" that could be used to make payments over the Internet or other electronic-mail systems.*

*The system would let a couple pay their phone bill by sending a payment to the telephone company over electronic mail, or they could send an **electronic check** to a child for a **birthday** present. A person or company receiving an **electronic check** could immediately deposit it in a bank, also via electronic mail.*

*"Anything you can do with a paper check you can do with an **electronic check** faster and cheaper," said John Doggett, a technology executive at Bank of Boston Corp. and head of the **electronic check** effort.*

Full Text:

Pretty soon it won't be, "The check is in the mail." It will be, "The check is in the E-mail."

A group of banks and technology companies said Tuesday that it would design a system to create "electronic checks" that could be used to make payments over the Internet or other electronic-mail systems.

The system would let a couple pay their phone bill by sending a payment to the telephone company over electronic mail, or they could send an electronic check to a child for a birthday present. A person or company receiving an electronic check could immediately deposit it in a bank, also via electronic mail.

"Anything you can do with a paper check you can do with an electronic check faster and cheaper," said John Doggett, a technology executive at Bank of Boston Corp. and head of the electronic check effort.

Unlike the electronic bill-payment services increasingly offered by banks, electronic checks could be sent directly by customers to their recipients, without going through the bank.

The electronic check would contain all the information that is on today's paper checks, including the bank issuing the check, an account number, an amount and the name of the person or organization receiving the payment. In addition, the check would contain a "digital signature," a security code that could prove that the check was authorized by the account holder.

To use the system, consumers would need an "electronic checkbook," a card that would be inserted into a slot on

their computers. The card, which is expected to cost $30 to $40 wholesale, would be required to verify the identity of the check writer and to prevent forgeries.

The group members hope the electronic checkbook will use the standard format, known as PC Card, that is used for modems and other accessories on most laptop computers. Later, the checkbook might fit onto credit card-sized "smart cards."

The project is at an early stage, and such issues as pricing have not been determined. The group hopes to set up a small test with fewer than 1,000 participants next year.

The consortium developing the electronic check consists of seven banks, including Citibank, the Bank of America and Chemical Bank; seven technology companies, including IBM and National Semiconductor Corp.; and four research organizations, including Bellcore and the University of Southern California.

It was organized by the Financial Services Technology Consortium, an industry group that intends to publish an open standard for electronic checks.

This electronic check project is just one of many initiatives to create computerized versions of various payment methods. Visa USA, Mastercard International and Microsoft Corp. are working on secure standards for sending credit-card numbers over the Internet.

Bank-technology group moves closer to cyberfinance Consortium writes, sends check over net

Boston Globe (Pre-1997 Fulltext); Boston, Mass.; Sep 22, 1995; Jon Auerbach, Globe Staff;

Sub Title: [City Edition]
Start Page: 39
ISSN: 07431791

Abstract:
Yesterday, a high-profile consortium of US banks and technology firms successfully wrote and sent a check over the Internet, touting the cyberpurchase as the first public demonstration of real money being moved from one account to another.

*The digital transaction came in the form of a $24.95 order for a So Soft teddy bear from PC **Gifts** & Flowers, a company that sells over the Internet.*

*Yesterday's demonstration came three months after the Financial Services Technology Consortium began its **Electronic Check** Project, with the aim of creating an viable infrastructure to support **electronic checks** and a host of other financial transactions that will be sent digitally.*

Full Text:

PLUGGED IN

The check is in the mail.

E-mail, that is.

Yesterday, a high-profile consortium of US banks and technology firms successfully wrote and sent a check over the Internet, touting the cyberpurchase as the first public demonstration of real money being moved from one account to another.

The digital transaction came in the form of a $24.95 order for a So Soft teddy bear from PC Gifts & Flowers, a company that sells over the Internet.

The bear was sent to Vice President Al Gore.

"We actually moved money with it," chirped Frank Jaffe, a senior systems consultant at the Bank of Boston Corp., a member of the consortium. "It's real."

Yesterday's demonstration came three months after the Financial Services Technology Consortium began its Electronic Check Project, with the aim of creating an viable infrastructure to support electronic checks and a host of other financial transactions that will be sent digitally.

The 21 FSTC companies involved in the checking project include banks such as Bank of Boston, Citicorp, and BankAmerica Corp., computer firms such as IBM Corp., Sun Microsystems Inc., and technology firms such as BBN Inc. of Cambridge and Telequip Corp. of Nashua.

Financial transactions conducted over the Internet have not met analysts' expectations, in part because of concerns over fraud felt by computer users.

The financial services consortium has stressed the security measures that are currently being developed for its electronic checkbook.

They include advanced cryptography to scramble information and personal "firewalls" that keep intruders out of private Internet sites.

According to Jaffe, the consortium's product is very much like a paper checkbook.

About the size of a thick credit card, the electronic checkbook will be issued to customers by banks, Jaffe said. The checkbook is "unlocked" with a password that allows it to communicate with either a chip inside the PC or a "smart card," a credit card with a built-in computer chip for authorization.

Jaffe said that most PCs will ship with hardware required to conduct such transactions within two years.

In yesterday's demonstration, a blue check appeared on the screen of the computer, which was set up inside a BankAmerica building in San Francisco.

Once the flower shop's Internet address was reached, the user at BankAmerica provided information on where to send the teddy bear.

Pressing a button on the electronic checkbook "signed" the check and sent it to the electronic boutique.

The money for the purchase was instantly taken from the consortium's account at Chemical Bank, Jaffe said.

It was unclear, however, whether the bear would arrive in Washington as quickly.

```
  SHOW FILES
File  47:Gale Group Magazine DB(TM) 1959-2003/Feb 21
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/Feb 21
         (c)2003 The Gale Group
File  16:Gale Group PROMT(R) 1990-2003/Feb 21
         (c) 2003 The Gale Group
?


Set     Items   Description
S1       3328   ELECTRONIC () CHECK
S2        822   S1 AND (BIRTHDAY OR CHRISTMAS OR GIFT OR GIVE OR PRESENT)
S3        144   S2 AND ((GIVE OR GIFT) (S) (ELECTRONIC () CHECK))
S4         51   S3 NOT PY>1999
S5          0   S4 AND ((ELECTRONIC (5N) GREETING))
S6        755   S1 AND ((CARD OR GREETING OR GIFT) (5N) (ELECTRONIC OR VIR-
            TUAL))
S7        755   S6 AND ((VIRTUAL () CHECK) OR (ELECTRONIC () CHECK))
S8      19302   ((CARD OR GREETING OR GIFT) (5N) (ELECTRONIC OR VIRTUAL))
S9          0   S8 AND ("ELECTRONIC CHECK")
S10       755   S8 AND (ELECTRONIC () CHECK)
S11        79   S10 AND GIFT
S12        10   S11 NOT PY>1999
S13         0   "E-GREETING"
S14         0   (E-GREETING?)
?
```